IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 9, 2020, accepted May 25, 2020, date of publication June 5, 2020, date of current version June 22, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3000231

Jitter-Quantizing-Based TRNG Robust Against PVT Variations

YINGCHUN LU[1], HUAGUO LIANG[1], LIANG YAO[1], XINYU WANG[1], HAOCHEN QI[1], MAOXIANG YI[1], (Associate Member, IEEE), CUIYUN JIANG[2], AND ZHENGFENG HUANG[1]

[1]School of Electronic Science and Applied Physics, Hefei University of Technology, Hefei 230009, China
[2]School of Mathematics, Hefei University of Technology, Hefei 230009, China

Corresponding author: Zhengfeng Huang (huangzhengfeng@139.com)

This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant 61674048, Grant 61574052, and Grant 61834006, and in part by the Science and Technology on Electronic Test and Measurement Laboratory of China under Grant 61420010202717.

ABSTRACT Security is critical to the growing popularity of the Internet of Things(IoT), and true random number generator (TRNG) plays an increasingly important role in information security systems. Conventional TRNGs use natural physical stochastic processes including thermal noise, chaos-based circuit, and so on to generate random numbers. These analog circuits based TRNG structures often consume excessive hardware resources. Meanwhile, it is difficult to incorporate them into digital system. In this paper, a novel all-digital true random number generator in SRAM-based FPGAs is proposed by using Vernier technique that precisely quantize random edge jitter. The proposed TRNG design is implemented on Xilinx Virtex-6 XC6VLX240T-1FF1156 FPGA and shows a high quality of randomness which has passed the NIST test suite with relatively high p-values, achieves a high throughput of 127 Mbps with occupying 32 slices. Experimental results show a good tolerance to bias phenomenon induced by process, voltage, and temperature variations.

INDEX TERMS True random number generator, Vernier technique, field programmable gate array, high throughput.

I. INTRODUCTION

Random number generator (RNG) is a key component in many security systems. They have been extensively used for key generation, authentication protocols, random padding, and so on. True random number generator (TRNG) is a kind of RNG that generates unpredictable bits, as opposed to pseudo random number generator (PRNG) which only provides a strong but completely predictable sequence of bits [1]–[4].TRNG utilizes uncertain random process (usually in the form of electronic thermal noise) as random entropy source, and adopts the mechanism of extracting entropy source (noise) to obtain random bit stream. TRNG generates unpredictable, statistically uniform, and non-repeatable true random numbers, which are widely used in social, industrial and scientific research fields, especially in the applications of modern science and technology [5], [6]. TRNG plays a significant role in communication security, cryptography, and Monte Carlo simulation. As a basic security module, TRNG has a vital impact on the sensitivity of security algorithms and the vulnerability of encryption systems, which has attracted more and more attention from academia and business circles [5]–[9].

TRNG designs extracting random numbers from thermal noise can be divided into analog TRNGs [10]–[12] and digital TRNGs [13]–[18]. Due to apparent advantages in cost saving, system integration, and technology portability compared to analog TRNGs, all-digital TRNGs (comprising solely digital components) have been comprehensively studied during last two decades. Typical all-digital TRNGs are mainly classified into ring oscillator (RO) based TRNG and metastability based TRNG [19], [20]. For RO-based TRNG, throughput is usually reduced due to timing jitter in a free-running RO as a source of randomness [21]–[23]. In order to improve throughput, the work in [14] sampled multiple parallel ROs while sacrificing area efficiency. Since unbiased physical source is difficult

The associate editor coordinating the review of this manuscript and approving it for publication was Yassine Maleh.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

to achieve, the metastability based TRNG [15] are always accompanied with severe bias phenomenon (statistical imbalance of '0' and '1') and each bias might adversely affect the extracted randomness.

To effectively improve randomness extraction, in this paper, instead of increasing the number of transition events (jitter accumulation), we generate random bits from a single propagation event (jitter quantization). Based on extremely small Vernier interval, a novel all-digital TRNG in field programmable gate arrays (FPGAs) is proposed, which effectively improves entropy extraction efficiency due to digitally snapshot random distribution of thermal noise jitter. Furthermore, the proposed TRNG have a good tolerance to bias phenomenon induced by process, voltage, and temperature (PVT) variations in FPGAs because of high quantization precision.

The rest of the paper is organized as follows. Section II introduces random jitter and the principle of jitter quantization. Section III presents the proposed small delay difference implementation, random entropy source model and the TRNG implementation. Experimental results are given in Section IV. Section V concludes this paper.

II. PRELIMINARIES

A. RANDOM JITTER

Jitter is defined as the deviation of the timing event of the signal from its ideal position. According to the type of jitter classification, it can be divided into deterministic jitter and random jitter. Deterministic jitters such as periodic jitter, data dependent jitter, and duty-cycle dependent jitter are essentially reproducible and predictable jitters [24]. Due to the peak-to-peak(pk-pk) value of deterministic jitter has upper and lower limits, on the basis of a relatively small number of observations, its boundary can usually be predicted with high confidence. For random jitter, in the circuit, the main source of random noise is thermal noise, and thermal noise exhibits a Gaussian distribution. For the peak of the Gaussian distribution is infinite, there is no peak-to-peak boundary value, and it cannot be accurately predicted. Random jitter refers to the timing variation caused by factors such as temperature and voltage that can affect the carrier mobility of semiconductor crystal materials and variations in semiconductor processing processes leading to uneven density of doping. As shown in Fig. 1, the jitter in digital circuits may be caused by power supply variations, temperature variations and propagation delays and it can be used to generate true random bit streams through D flip-flop (DFF) based samplers for sampling the output of the high frequency [25], as illustrated in Fig. 2.

B. JITTER QUANTIZATION

The main principle of the proposed jitter quantization is based on the high precision time-to-digital conversion (TDC) [26] using Vernier technology. Based on Vernier technique, we implement pulse measurement circuit in Xilinx Virtex-6 XC6VLX240T-1FF1156 (ML 605) FPGA in [27], [28].

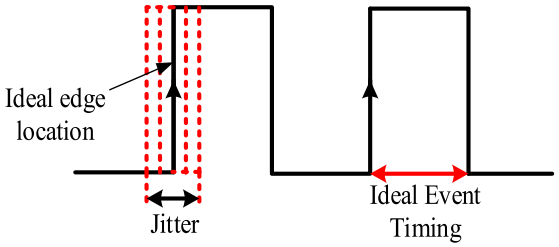


FIGURE 1. Jitter in digital circuit.

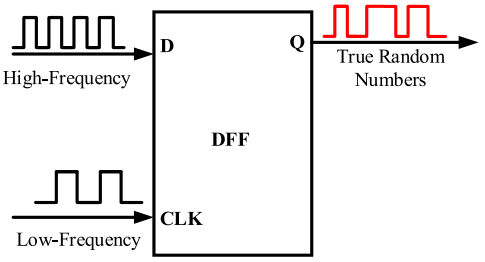


FIGURE 2. Basic TRNG based DFF.

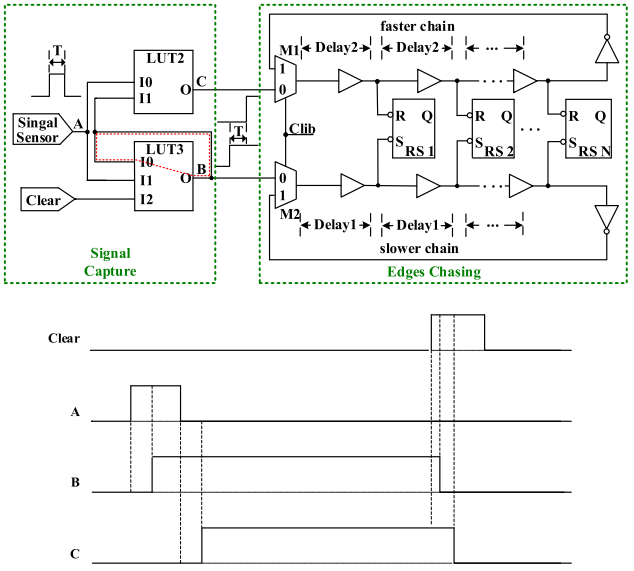


FIGURE 3. Pulse measurement circuit in [22].

As shown in Fig. 3 presented in [27], the pulse measuring circuit mainly consists of two parts, i.e., signal capture part and edges chasing part. The measured pulse(T) is captured by LUT3 (3-input LUT) and then driven by two positive edges to propagate through two chains within the time interval of the pulse width. Since the two chains have different propagation delays in advance, the edges of the faster chain will chase the other edges in the slower chain, so the pulse width can be determined: the Vernier interval (Delay1-Delay2) multiplied by the number of propagation stages required for the two chains to meet.

As known from experimental results in [28], the edges chasing part is able to quantize pulse width with a good accuracy. Obviously, reducing the Vernier interval can further improve the conversion accuracy (optimized to 30 ps in [28]). However, this optimization trend is unsustainable because there is jitter during edge propagation due to electronic

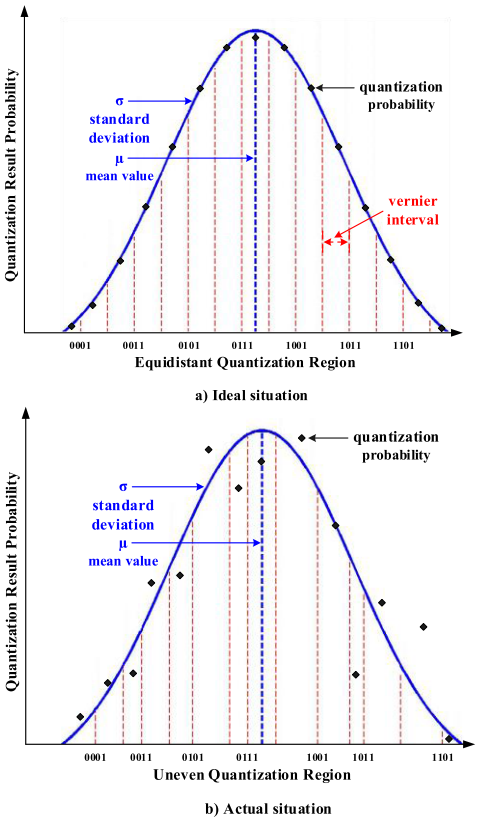


FIGURE 4. Jitter quantization.

thermal noise. As the Vernier interval value (quantization accuracy) gradually increases, the improvement in pulse measurement accuracy is greatly weakened or even invalid, but the edge Jitter can be quantified with high accuracy. As shown in Fig. 4, if the Vernier interval remains reduced until the value of the Vernier interval is much smaller than the magnitude of the thermal noise jitter, the conversion result will become uncertain due to some fluctuations in the LSB in the quantization result [29]. Obviously, the uncertainty is exactly the result of the quantification of thermal noise. In other words, when the Vernier interval is small enough, the Vernier circuit can be used to quantify the random edge jitter. In the ideal case of equidistant Vernier interval as shown in Fig. 4a, the quantization results will approximately follow a Gaussian distribution $N(\mu, \sigma 2)$, where μ is the result of the conversion without thermal noise and σ is the standard deviation of the quantized values of accumulated thermal jitter under edge propagation. The Vernier interval is very uneven due to system delay mismatch caused by PVT variations, as shown in Fig. 4b. The extremely high precision of the jitter quantization will also effectively prevent the quality degradation of the extracted entropy caused by the bias phenomenon.

III. TRNG ARCHITECTURE

A. SMALL DELAY DIFFERENCE IMPLEMENTATION

Fig. 5a demonstrates a look up table (LUT, the basic configurable cell in SRAM-based FPGAs) structure. Operation principles of such structure are as follows: when a set of

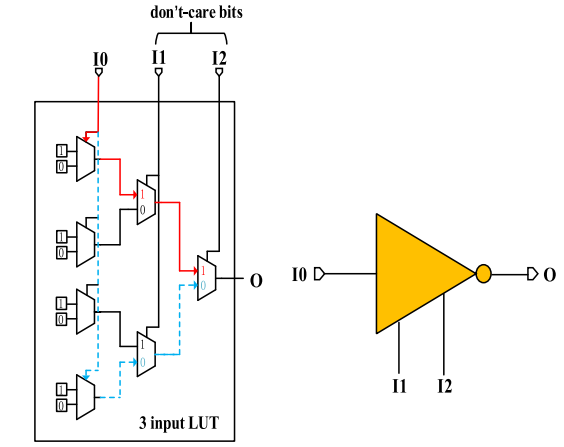


FIGURE 5. LUT_3 structure and inverter schematic with don't-care bit.

path gated signals (I0, I1, I2) input, LUT output is directly connected to a SRAM cell and then determined by the conducting SRAM cell. Therefore, by configuring corresponding values to SRAM cells, a combinational logic function with three or less inputs can be implemented in LUT_3. Different inputs result in different conducting paths (multiple factors including transistor type, placement, and routing may change), which presents different LUT delays.

As shown in Fig. 5, the LUT is configured so that the inputs I1 and I2 act as don't-care bits while I0 acts as signal bit. The LUT output O is a logical NOT of I0 and are independent of I1 and I2. For instance, if I1I2 = 00, the signal propagates through the blue dashed-lines, and when I1I2 = 11, the signal propagates through the path with the red solid path marked. Obviously, the dashed path is slightly longer than the red solid path, which results in a larger propagation delay.

Inspired by this phenomenon, we propose a high-precision delay adjustment method, whose basic idea is to fine-tune the path delay by configuring the internal signal propagation path of the LUT [27]. In order to obtain the desired delay difference (less than or equal to 1 ps), a delay-time adjustable transmission gate [27] is constructed, which includes a signal port and a delay adjustment port. The results of previous experiments in [27] show that one LUT physical port (A1, A2,...,A5,A6) can be mapped arbitrarily to one of I0, I1, I2 logical ports of the LUT. To minimize the impact of process fluctuations on TRNG and maximize TRNG throughput, A5 is configured as signal port and the delay adjustment port is set to A4 or A6 adjacent to the signal port. In order to determine the amount of delay that the A4 and A6 ports affect the circuit, as shown in Fig. 6, 12 such transmission gates and one NAND gate are connected to form a RO. Then any one node on this RO is connected to a rising edge of a sufficiently large range counter, and other one node is connected to a rising edge sensitive clock of a large enough counter. By counting the number of rising edges that propagate through the node for a specific time T, we can calculate the delay of the RO:

$$RO_{delay} = 2 * \frac{T}{Number_{counter}} \quad (1)$$

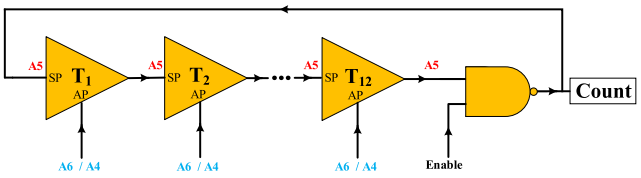


FIGURE 6. Measurement circuit for A4 and A6.

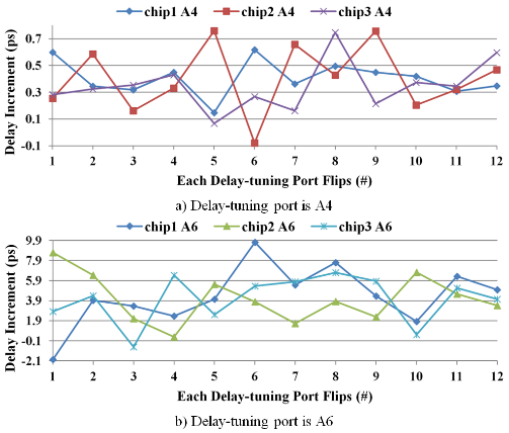


FIGURE 7. Tunable delay for A4 and A6.

where $Number_{counter}$ is the number of rising edges remembered during T. Whenever the logic state of the delay adjustment port is inverted, we can obtain a new RO delay, which is the adjustable delay amount relative to the time of the old RO delay.

In the experiment, we conducted delay adjustment evaluation under three ML605 platforms. With two delay adjustment cases, we can get a total of 72 delay increments. As shown in Fig. 7, the average delay increment is approximately 0.37 ps when the delay adjustment port is A4, and the average delay increment is approximately 4.2 ps when the delay adjustment port is A6. It can be seen that the delay adjustment method for configuring the internal path of the LUT can well meet the delay difference requirement of the proposed TRNG.

B. RANDOM ENTROPY SOURCE MODEL

Through the pre-working TDC technology [27], N cycles of ring i catch up to $N+1$ cycles of ring j without jitter, e.g.,

$$\sum_{i=0}^{N} T_i - \sum_{i=0}^{N+1} T_j = 0 \tag{2}$$

where T_i is the ring i oscillation period, and the ring j oscillation period is T_j.

Assuming that the width of each jitter is x, it can be seen that after the jitter occurs, the length of the difference y between the ring i after N cycles and the ring j after $N+1$ cycles. Due to the presence of thermal noise, the difference y will vary with any jitter. This design extracts the difference y as the source of TRNG random entropy.

According to the [30], the occurrence probability of the width $x \in (-p, p)$ is different when any jitter occurs,

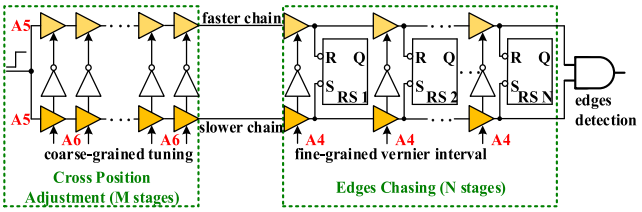


FIGURE 8. The proposed TRNG.

and its probability follows the normal distribution $g(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$, then the average width of jitter occurrence in N cycles should be $EX = xg(x)$, that is, the distribution law y of the difference is:

$$\begin{aligned} y &= \left| \sum_{i=0}^{N} \left(T_i + x_i g\left(x_i\right)\right) - \sum_{j=0}^{N+1} \left(T_j + x_j g\left(x_j\right)\right) \right| \\ &= \left| \sum_{i=0}^{N} x_i g\left(x_i\right) - \sum_{j=0}^{N+1} x_j g\left(x_j\right) \right| \end{aligned} \tag{3}$$

If $xi, xjx_{i,}x_j$ is rearranged and named $x0 \sim \boldsymbol{xn}x_0 \sim x_n$ in ascending order, then the result of the formula (3) y has not changed after reordering, i.e., y is:

$$y = \left| \sum_{i=0}^{N} \left[x_i g\left(x_i\right) - x_j g\left(x_j\right)\right] - x_{n+1} g\left(x_{n+1}\right) \right| \tag{4}$$

Since the jitter width itself is small enough, when the catch-up period is long enough, the reordered $x_i \to x_j$, e.g., $\left(x_i - x_j\right) \to \mathbf{0}$. Then $g\left(x_i\right) \approx g\left(x_j\right)$, let $g\left(\boldsymbol{\xi}\right) = \frac{g(x_i)+g(x_j)}{2}$. Formula (4) is changed to:

$$\begin{aligned} y &= \left| \lim_{(x_i - x_j) \to 0} \sum_{i=0}^{N} \left(x_i - x_j\right) g\left(\xi\right) - x_{n+1} g\left(x_{n+1}\right) \right| \\ &= \int_{x_0}^{x_n} g\left(x\right) dx - x_{n+1} g\left(x_{n+1}\right) \end{aligned} \tag{5}$$

It can be seen from formula (5) that the distribution law of the difference value follows the normal distribution law, that is, the difference value is random.

C. TRNG IMPLEMENTATION

Based on the above-mentioned adjustable transmission gate, as shown in Fig. 8, we implement a TRNG on the Xilinx FPGA, and the TRNG circuit is mainly divided into two parts, eg., the cross position adjustment and the edge chasing. Based on the finer-grained Vernier interval (adjustment port A4, approximately 0.74 ps, double 0.37 ps), time-to-digital converter (TDC) can digitize the random edge jitter of electronic thermal noise at the edge chasing portion. By dynamically configuring the set values in the coarse grain (adjustment port A6, each set value corresponds to 8.4 ps), we can compensate or correct the quantized center position offset (edge chasing part) caused by the PVT variations in real time. In the experiment, the cross-position adjustment portion can cause the most likely position of the edge intersection to be at or near the center of the edge chasing portion, ensuring a stable and high-quality entropy extraction efficiency [31].

TABLE 1. NIST SP800-22, randomness test result of multiple chips (20 °C, 1.0 V).

NIST SP800-22 Test	Chip#1		Chip#2		Chip#3	
	P-value	Proportion	P-value	Proportion	P-value	Proportion
Approximate Entropy	**0.709096**	60/60	**0.925760**	60/60	**0.503508**	60/60
Block Frequency	**0.791345**	60/60	**0.530228**	60/60	**0.582456**	60/60
CumulativeSums0	0.570353	60/60	0.987745	60/60	0.743471	60/60
Cumulative Sums1	0.495741	60/60	0.972916	60/60	0.695963	60/60
FFT	0.561658	60/60	0.222920	60/60	0.353091	60/60
Frequency	0.431044	60/60	0.959647	60/60	0.701990	60/60
Linear Complexity	0.309326	60/60	0.246048	60/60	0.850579	60/60
Longest Run	0.661546	60/60	0.566880	60/60	0.431795	60/60
Overlapping Template	0.492608	60/60	0.956764	60/60	0.799989	60/60
Rank	0.294391	60/60	0.807360	60/60	0.643341	60/60
Runs	0.442811	60/60	0.597432	60/60	0.193626	60/60
Serial0	**0.859383**	60/60	**0.927355**	60/60	**0.683902**	60/60
Serial1	**0.595189**	60/60	**0.722709**	60/60	**0.734164**	60/60
Universal	**0.643020**	60/60	**0.592236**	60/60	**0.989128**	60/60
Non Overlapping Template	0.485156	60/60	0.518914	60/60	0.537440	60/60
Random Excursions	0.458625	60/60	0.468866	60/60	0.726773	60/60
Random Excursions Variant	0.625066	60/60	0.332965	60/60	0.522032	60/60

* For Non overlapping template, Random excursions variant and Random excursions, the P-value is the average of the P-values of all the sub-tests of the test.

In this TRNG implementation, the actual output latency of each transmission gate is T: approximately 247 ps, which is the sum of 177 ps (line delay, nominally 294 ps on the static timing analysis report, based on empirical values,Virtex6 FPGA Timing Characteristics Data Sheet [32]) and 70 ps (LUT delay according to [33]).

As shown in Fig. 8, in the entire TRNG Vernier circuit, the values of M and N are 6 and 26, respectively, for a total of 32 levels, so we can determine the operating period(OP) of the TRNG:

$$OP = 2 * (T * (M + N)) \tag{6}$$

Substitute the experimental data into the formula, the operating period(OP) of the trng is 15.8 ns. In the process of random number extraction, the quantitative results of electron thermal noise are analyzed deeply and it is found that the lowest two significant bits have good randomness.

Therefore, we use a simple and effective method to generate true random numbers, which is the output quantization result. The lowest two valid bits divided by 15.8 ns is equal to 127 Mbps, which in the throughput of the proposed TRNG.

IV. EXPERIMENTAL RESULTS

In our experiment, the TRNG is implemented in three Xilinx Virtex-6 FPGAs and multiple operating conditions (changing the temperature from 20 degrees Celsius to 80 degrees Celsius in 20 degrees Celsius steps and the core voltage from 0.8 V to 1.2 V in 200 mV steps). In each case, 1 Mb raw data are extracted and then evaluated by NIST SP800-22 RNG test suite (15 random tests) [34] and NIST SP800-90B RNG test suite [35].

A. NIST SP800-22 RNG TEST

1) RANDOMNESS AND PERFORMANCE OF THE TRNG FOR MULTIPLE CHIPS

1 Mb raw data are generated by the proposed TRNG under normal circumstances (20°C, 1.0V) to pass NIST randomness test. P-value is an index which indicates the randomness quality of a sequence. When P-value is greater than 0.01, randomness is acceptable. The tests are executed on three ML605 FPGAs for sixty times. The results are shown in Table 1, the random bitstreams can pass all the randomness tests and have relatively high P-value. More strikingly, the P-value of Approximate Entropy, Block Frequency, Universal, Serial0, and Serial1 tests exceeds 0.5, so the generated key sequence is random [36], in other words, the proposed TRNG can be used as a safety device.

2) RELIABILITY TEST OF THE TRNG INDUCED BY PVT

Digital TRNG has the advantage of easy integration and less sensitive to process, voltage, and temperature changes (PVT changes) [37,38] compared to traditional analog design. For mobile and Internet of Things (IoT) applications, the environmental robustness of TRNG become very important. Thus, some experiments are conducted, in which random bitstreams are generated by the proposed TRNG structure under different environments (temperatures: 20 °C ∼ 80 °C) and different operation voltages (0.8 V ∼ 1.2 V).

The results are also tested to verify the reliability of the proposed TRNG. As shown in Table 2 and Figure 8, while diversification in voltage and temperature affects the quality of random bitstreams, the results can still pass all tests with quite high p-value in the NIST statistical test suite.

It is worth noting that, as shown in Figure 9, at 80 °C extreme temperature, the proposed TRNG can pass the test

TABLE 2. NIST SP800-22 statistical test result of PVT.

NIST SP800-22 Test	20			40			60		
	Voltage/V			Voltage/V			Voltage/V		
	0.8	1	1.2	0.8	1	1.2	0.8	1	1.2
	P-value			P-value			P-value		
Approximate Entropy	0.9100	0.7091	0.8206	0.6411	0.7351	0.6703	0.9085	0.8603	0.5891
Block Frequency	0.7513	0.7913	0.9912	0.7697	0.9705	0.8343	0.9670	0.6391	0.9989
Cumulative Sums0	0.8397	0.5704	0.6974	0.9903	0.8982	0.7976	0.8189	0.5125	0.5745
Cumulative Sums1	0.8090	0.4957	0.3253	0.9654	0.3619	0.5471	0.8571	0.2486	0.4523
FFT	0.2175	0.5617	0.6845	0.6529	0.6739	0.1772	0.9537	0.7386	0.9537
Frequency	0.7185	0.4310	0.3675	0.9345	0.5230	0.5354	0.7590	0.3542	0.8818
Linear Complexity	0.1399	0.3093	0.2408	0.5917	0.9846	0.6196	0.5921	0.7909	0.4202
Longest Run	0.2823	0.6615	0.1245	0.8943	0.8532	0.3943	0.9822	0.8817	0.3335
Overlapping Template	0.7077	0.4926	0.4591	0.5947	0.7428	0.1085	0.3527	0.7280	0.1109
Rank	0.8049	0.2944	0.5916	0.2607	0.1140	0.4156	0.3515	0.3675	0.7233
Runs	0.6742	0.4428	0.0438	0.5974	0.1362	0.3361	0.5374	0.3732	0.4807
Serial0	0.6244	0.8594	0.9295	0.2278	0.5971	0.8725	0.7428	0.8758	0.2397
Serial1	0.7101	0.5952	0.6172	0.2866	0.2252	0.9644	0.6689	0.9057	0.3324
Universal	0.8819	0.6430	0.3428	0.3718	0.4972	0.8659	0.9993	0.6992	0.4010
Non Overlapping Template	0.5411	0.4852	0.5173	0.4996	0.4551	0.4941	0.4974	0.4890	0.4948
Random Excursions	0.3294	0.4586	0.5394	0.5542	0.4634	0.4812	0.6177	0.4072	0.4897
Random Excursions Variant	0.4715	0.6251	0.6600	0.4375	0.6287	0.3504	0.5240	0.6886	0.6795

* For Non overlapping template, Random excursions variant and Random excursions, the P-value is the average of the P-values of all the sub-tests of the test.
* For each group of tests, 60 experiments were carried out. The P-value in the table was 60 times average, and the passing rate was over 99%.

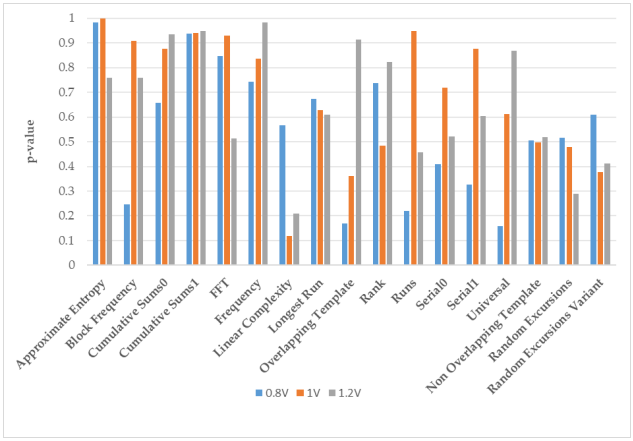


FIGURE 9. NIST SP800-22 statistical test results at 80 °C.

with a P-value greater than 0.1. It indicates that the proposed true random number generator structure can produce high-quality random numbers with high efficiency and be affected slightly by the temperature and voltage.

B. NIST SP800-90B RNG TEST

Note that NIST SP800-22 is a statistical test suite for random and pseudo random number sequences, while NIST SP800-90B is an entropy estimation method used to verify the quality of the output entropy source of non-deterministic processes. Since the TRNG proposed in this paper is a non-deterministic process, it is appropriate to use NIST SP 800-90B to test the statistical properties of its output sequence. NIST SP 800-90B is used for entropy evaluation of noise sources. Entropy evaluation involves two steps: determining the track (Independent and Identically Distributed (IID) or non-IID) and estimating the entropy of a given original random sequence.

In order to steadily determine the distribution of the original random sequence, the length of the test sequence needs 1 Mb raw data. In order to test the stability of the entropy of the proposed TRNG in harsh environments, we randomly selected five generation sequences of TRNG working at 80 °C for NIST SP800-90B test. According to the experimental test results, it can be shown that the five randomly selected sequences have passed the IID test (including chi-square independence test, chi-square goodness-of-fit test, longest repeated substring (LRS) test), non-IID test, and restart test. Table 3 shows the results of NIST SP800-90B entropy estimation under non-IID test on the original sequences. It can be shown that the original sequences passed non-IID test of the NIST SP800-90B test. And the min-entropy of all raw sequences is determined by collision estimation [35], and the entropy rates are stable with an average value of 0.9314508.

TABLE 3. Entropy rate of proposed TRNG sequences.

Non-IID Test	Sequence1	Sequence2	Sequence3	Sequence4	Sequence5
MCV	0.995621	0.994813	0.995860	0.996044	0.995747
Collision	0.966577	0.933911	0.888864	0.944718	0.923184
Markov	0.994598	0.995933	0.997266	0.995483	0.95597
Compression	1	1	1	1	1
t-tuple	0.946909	0.941613	0.922601	0.922601	0.925141
LRS	0.997547	0.999993	0.994676	0.994666	0.998274
Multi-MCW	0.998519	0.995674	0.996675	0.997061	0.996756
Lag	0.994547	0.925560	0.996860	0.994159	0.995720
Multi-MMC	0.995319	0.994928	0.996346	0.999215	0.995693
LZ78Y	0.994170	0.995122	0.997249	0.995208	0.995182

TABLE 4. Comparison with related work.

Work	Platform	Resources	Special Modules	Throughput (Mb/s)
[23]	Virtex-5	128 slices	no	100
[30]	Virtex-2 pro	565 slices	no	2.5
[31]	Spartan 6	67 slices	no	14.3
[39]	Virtex-5	40 slices	DCM	<1
[40]	Spartan 3A	270 slices	no	6
This work	Spartan 6	**32 slices**	**no**	**127**

C. COMPARISON WITH RELATED WORKS

Comparison with the related work [23], [30], [31], [39] and [40], as shown in Table 4, the proposed TRNG design achieves a higher throughput of 127 Mbps while occupying lower resource overhead and improving randomness extraction in FPGAs. It is worth mentioning that the throughput of the proposed TRNG is hardly affected by temperature and voltage after lots of experiments.

V. CONCLUSION

Randomness is crucial for TRNG, and the keys generated by TRNG with superior randomness are more secure. To effectively improve randomness of entropy extraction, a novel all-digital TRNG on FPGAs is proposed in this paper, based on extremely small Vernier interval. Our design can digitally snapshot random distribution of thermal noise jitter, improving entropy extraction efficiency and quantization precision of the TRNG.

Experimental results shows that the TRNG design in this paper is able to generate high-quality random bits with high throughput and good reliability against PVT variations.

ACKNOWLEDGMENT

The authors thank Prof. Z. Huang and Prof. H. Liang for their useful discussions.

REFERENCES

[1] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Cryptanalytic attacks on pseudorandom number generators," in *Proc. Int. Workshop Fast Softw. Encryption*. Berlin, Germany: Springer, 1998, pp. 168–188.
[2] A. Sidorenko and B. Schoenmakers, "State recovery attacks on pseudorandom generators," in *Proc. WEWoRC*, Leuven, Belgium, 2005, pp. 53–63.
[3] A. B. O. Lopez, L. H. Encinas, A. M. Munoz, and F. M. Vitini, "A lightweight pseudorandom number generator for securing the Internet of Things," *IEEE Access*, vol. 5, pp. 27800–27806, 2017.
[4] V. L. Shrestha, Q. Ma, M. P. Haider, and Y. Massoud, "An ultra-low-power pseudo-random number generator based on biologically inspired chaotic silicon neuron circuit," *IEICE Electron. Express*, vol. 9, no. 22, pp. 1756–1761, 2012.
[5] V. von Kaenel and T. Takayanagi, "Dual true random number generators for cryptographic applications embedded on a 200 million device dual CPU SoC," in *Proc. IEEE Custom Integr. Circuits Conf.*, Sep. 2007, pp. 269–272.
[6] K. Lee, S.-Y. Lee, C. Seo, and K. Yim, "TRNG (true random number generator) method using visible spectrum for secure communication on 5G network," *IEEE Access*, vol. 6, pp. 12838–12847, 2018.
[7] D. Liu, Z. Liu, L. Li, and X. Zou, "A low-cost low-power ring oscillator-based truly random number generator for encryption on smart cards," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 63, no. 6, pp. 608–612, Jun. 2016.
[8] K. Nohl, D. Evans, S. Starbug, and H. Plötz, "Reverse-engineering a cryptographic RFID Tag," in *Proc. USENIX Secur. Symp.*, Berkeley, CA, USA, 2008, pp. 185–193.
[9] Q. Zhou, X. Liao, K.-W. Wong, Y. Hu, and D. Xiao, "True random number generator based on mouse movement and chaotic hash function," *Inf. Sci.*, vol. 179, no. 19, pp. 3442–3450, Sep. 2009.
[10] I. Cicek, A. E. Pusane, and G. Dundar, "A novel design method for discrete time chaos based true random number generators," *Integration*, vol. 47, no. 1, pp. 38–47, Jan. 2014.

[11] K. Yang, D. Fick, M. B. Henry, Y. Lee, D. Blaauw, and D. Sylvester, "A 23Mb/s 23pJ/b fully synthesized true-random-number generator in 28 nm and 65 nm CMOS," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, San Francisco, CA, USA, Feb. 2014, pp. 280–281.

[12] S. Callegari and G. Setti, "ADCs, chaos and TRNGs: A generalized view exploiting Markov chain lumpability properties," in *Proc. IEEE Int. Symp. Circuits Syst.*, New Orleans, LA, USA, May 2007, pp. 213–216.

[13] F. Ouattara, A. Nejat, L. Torres, and K. Mackay, "Practical experiments on fabricated TAS-MRAM dies to evaluate the stochastic behavior of voltage-controlled TRNGs," *IEEE Access*, vol. 7, pp. 59271–59277, 2019.

[14] X. Wu and S. Li, "A new digital true random number generator based on delay chain feedback loop," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Baltimore, MD, USA, May 2017, pp. 1–4.

[15] S. K. Mathew, D. Johnston, S. Satpathy, V. Suresh, P. Newman, M. A. Anders, H. Kaul, A. Agarwal, S. K. Hsu, G. Chen, and R. K. Krishnamurthy, "μ RNG: A 300–950 mV, 323 Gbps/W all-digital full-entropy true random number generator in 14 nm FinFET CMOS," *IEEE J. Solid-State Circuits*, vol. 51, no. 7, pp. 1695–1704, Jul. 2016.

[16] L. T. Clark, S. B. Medapuram, and D. K. Kadiyala, "SRAM circuits for true random number generation using intrinsic bit instability," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 26, no. 10, pp. 2027–2037, Oct. 2018.

[17] S. Kiamehr, M. S. Golanbari, and M. B. Tahoori, "Leveraging aging effect to improve SRAM-based true random number generators," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Lausanne, Switzerland, Mar. 2017, pp. 882–885.

[18] V. V. Der Leest, E. V. Der Sluis, G. Schrijen, P. T. Tuyls, and H. Handschuh, "Efficient implementation of true random number generator based on SRAM PUFs," in *Cryptography and Security: From Theory to Applications*. Berlin, Germany: Springer, 2012, pp. 300–318.

[19] N. Fujieda and S. Ichikawa, "A latch-latch composition of metastability-based true random number generator for Xilinx FPGAs," *IEICE Electron. Express*, vol. 15, no. 10, May 2018, Art. no. 20180386.

[20] F. Mei, L. Zhang, C. Gu, Y. Cao, C. Wang, and W. Liu, "A highly flexible lightweight and high speed true random number generator on FPGA," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI (ISVLSI)*, Hong Kong, Jul. 2018, pp. 399–404.

[21] D. Schellekens, B. Preneel, and I. Verbauwhede, "FPGA vendor agnostic true random number generator," in *Proc. Int. Conf. Field Program. Log. Appl.*, Madrid, Spain, Aug. 2006, pp. 44–139.

[22] K. Wold and C. H. Tan, "Analysis and enhancement of random number generator in FPGA based on oscillator rings," in *Proc. Int. Conf. Reconfigurable Comput. FPGAs*, Cancun, Mexico, Dec. 2008, pp. 385–390.

[23] A. Cherkaoui, V. Fischer, L. Fesquet, and A. Aubert, "A very high speed true random number generator with entropy assessment," in *Proc. Int. Conf. Cryptograph. Hardw. Embedded Syst.*, Santa Barbara, CA, USA, 2013, pp. 179–196.

[24] K. Ichiyama, M. Ishida, T. J. Yamaguchi, and M. Soma, "Novel CMOS circuits to measure data-dependent jitter, random jitter, and sinusoidal jitter in real time," *IEEE Trans. Microw. Theory Techn.*, vol. 56, no. 5, pp. 1278–1285, May 2008.

[25] T. Amaki, M. Hashimoto, and T. Onoye, "An oscillator-based true random number generator with jitter amplifier," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2011, pp. 725–728.

[26] H. Menninga, C. Favi, W. F. Fishburn, and E. Charbon, "A multichannel, 10ps resolution, FPGA-based TDC with 300MS/s throughput for open-source PET applications," in *Proc. IEEE Nucl. Sci. Symp.*, Oct. 2011, pp. 1515–1522.

[27] H. Liang, X. Xu, Z. Huang, C. Jiang, Y. Lu, A. Yan, Y. Ouyang, M. Yi, and T. Ni, "A methodology for characterization of SET propagation in SRAM-based FPGAs," *IEEE Trans. Nucl. Sci*, vol. 63, no. 6, pp. 2985–2992, Dec. 2016.

[28] X. Xu, H. Liang, Z. Huang, C. Jiang, Y. Lu, A. Yan, and M. Yi, "A single event transient detector in SRAM-based FPGAs," *IEICE Electron. Express*, vol. 14, no. 12, pp. 1–6, Dec. 2017.

[29] M. Fishburn, L. H. Menninga, C. Favi, and E. Charbon, "A 19.6 ps, FPGA-based TDC with multiple channels for open source applications," *IEEE Trans. Nucl. Sci.*, vol. 60, no. 3, pp. 2203–2208, Jun. 2013.

[30] B. Sunar, W. Martin, and D. Stinson, "A provably secure true random number generator with built-in tolerance to active attacks," *IEEE Trans. Comput.*, vol. 56, no. 1, pp. 109–119, Jan. 2007.

[31] V. Rozic, B. Yang, W. Dehaene, and I. Verbauwhede, "Highly efficient entropy extraction for true random number generators on FPGAs," in *Proc. 52nd Annu. Design Autom. Conf. (DAC)*, San Francisco, CA, USA, 2015, pp. 1–6.

[32] Xilinx Corporation. (2014). *Virtex-6 FPGA Data Sheet: DC and Switching Characteristics [EB/OL]*. [Online]. Available: https://www.xilinx.com/support/documentation/data_sheets/ds152.pdf

[33] Xilinx Corporation. (2013). *Virtex-6 Libraries Guide for HDL Designs (UG623), v14.7*. [Online]. Available: https://www.xilinx.com/support/documentation/sw_manuals/xilinx14_7/virtex6_hdl.pdf

[34] NIST. (2010). *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf

[35] M. S. Turan, E. Barker, J. Kelsey, K. McKay, M. Boyle, and M. L. Baish, "NIST Special Publication 800-90B: Recommendation for the entropy sources used for random bit generation," U.S. Dept. Commerce, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. SP 800-90B, 2018.

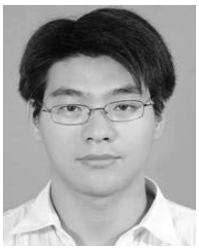
[36] L. Fan, H. Chen, and S. Gao, "A general method to evaluate the correlation of randomness tests," in *Proc. Int. Workshop Inf. Secur. Appl.* Cham, Switzerland: Springer, 2013, pp. 52–56.

[37] S. K. Mathew, S. Srinivasan, M. A. Anders, H. Kaul, S. K. Hsu, F. Sheikh, A. Agarwal, S. Satpathy, and R. K. Krishnamurthy, "2.4 gbps, 7 mW all-digital PVT-variation tolerant true random number generator for 45 nm CMOS high-performance microprocessors," *IEEE J. Solid-State Circuits*, vol. 47, no. 11, pp. 2807–2821, Nov. 2012.

[38] T. Amaki, M. Hashimoto, and T. Onoye, "A process and temperature tolerant oscillator-based true random number generator with dynamic 0/1 bias correction," in *Proc. IEEE Asian Solid-State Circuits Conf. (A-SSCC)*, Singapore, Nov. 2013, pp. 133–136.

[39] A. P. Johnson, R. S. Chakraborty, and D. Mukhopadyay, "An improved DCM-based tunable true random number generator for Xilinx FPGA," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 64, no. 4, pp. 452–456, May 2016.

[40] N. N. Anandakumar, S. K. Sanadhya, and M. S. Hashmi, "FPGA-based true random number generation using programmable delays in oscillator-rings," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 3, pp. 570–574, Mar. 2020.



YINGCHUN LU received the M.E. degree in microelectronics and solid-state electronics from the Hefei University of Technology, in 2005. His research interests include IC and FPGA application design.

HUAGUO LIANG was born in 1959. He received the Ph.D. degree in computer science from the University of Stuttgart, Germany, in 2003. From 1998 to 2003, he was a Research Fellow with the Department of Computer Science, University of Stuttgart. He is currently a Professor and a Ph.D. Supervisor with the School of Computer and Information and the School of Electronic Science and Applied Physics, Hefei University of Technology, Hefei, China. He is also the Dean with the School of Electronic Science and Applied Physics and the School of Microelectronics, Hefei University of Technology. He has taken charge of many projects, such as DFG, the National Natural Science Foundation, the Scientific Research Foundation for the Returned Overseas Chinese Scholars, and the State Education Ministry. He has published a book in Germany and more than 100 journal articles. His research interests include built-in-self-test, design automation of digital systems, ATPG algorithms, distributed control, and so on. He served as the General Chair on the Organizing Committee for the IEEE Asian Test Symposium, in 2018.

LIANG YAO received the B.S. degree in electronic engineering science and technology from Anhui Polytechnic University, in 2016. He is currently pursuing the Ph.D. degree in integrated circuit and system with the School of Electronic Science and Applied Physics, Hefei University of Technology, in 2017. His research interests include hardware security and IC design.

XINYU WANG received the bachelor's degree in electronic science and engineering from the Hefei University of Technology, in 2018, where he is currently pursuing the degree in integrated circuits. His main research interest includes hardware security.

HAOCHEN QI received the B.E. degree in industrial automation from the Anhui University of Technology, China, in 2003, and the M.Sc. degree in integrated circuit engineering from the Hefei University of Technology, China, in 2009, where she is currently pursuing the Ph.D. degree in integrated circuits and systems. Her research interests include IC test, quality control in semiconductor process, and biosensors.

MAOXIANG YI (Associate Member, IEEE) received the B.S. degree in semiconductor devices, the M.S. degree in microelectronics, and the Ph.D. degree in computer application technology from the Hefei University of Technology, Hefei, China, in 1986, 1989, and 2010, respectively. From 2002 to 2003, he was a Visiting Scholar with the Institute of Physical Electronics, University of Stuttgart, Stuttgart, Germany. He is currently a Professor and a master's Supervisor of electronic science and technology with the Hefei University of Technology. He has published more than 40 journal or conference papers. His research interests include very large-scale integrated circuit design for testability and reliability.

CUIYUN JIANG received the B.S. degree in mathematics from Anhui University, Hefei, China, in 1983, and the M.S. degree in computational mathematics from the Hefei University of Technology, Hefei, in 1987.

She is currently an Associate Professor with the School of Mathematics, Hefei University of Technology. She has published over 30 journal or conference papers. Her current research interests include mathematical modeling and VLSI test.

ZHENGFENG HUANG received the Ph.D. degree in computer engineering from the Hefei University of Technology, in 2009. He was a Visiting Scholar with the University of Paderborn, Germany, from 2014 to 2015. He is currently a Professor with the Hefei University of Technology. His current research interest includes design for soft error tolerance/mitigation. He is a member of the Technical Committee on Fault Tolerant Computing which belongs to the China Computer Federation. He served on the Organizing Committee of the IEEE European Test Symposium (ETS), in 2014. He was a Program Co-Chair of the IEEE Asian Test Symposium (ATS), in 2018.